32 Above n 22, 17.

33 Ibid.

34 Ibid.

35 Ibid.

36 Spam Act s 16.

37 CAN-SPAM Act § 5(a)(4).

38 Coalition Against Unsolicited Commercial Email, 'Statement on House Spam Bill Vote' (22 November 2003) <http://www.cauce.org/news>.

39 Elizabeth Alongi, 'Has the US Canned Spam?' 46 *Arizona Law Review* 263, 275, 287.

40 See <http://www.ftc.gov/opa/1999/12/oecdguide.htm>.

41 Sebastian Hughes, 'Avoiding the Toothless Tiger' – Effective Anti-Spam Legislation for Hong Kong' (2004) 58 *Intellectual Property Forum* 38, 41.

42 Jacquelyn Trussell, 'Is the CAN-SPAM Act the Answer to the Growing Problem of Spam?' (2004) 16 *Loyola Consumer Law Review* 175, 187.

43 John Corker, 'Scams and legal approaches to spam' (2002) 5(6) *Internet Law Bulletin* 61, 67.

44 Above n 38.

45 Trussell, above n 42, 183.

46 Australian Communications and Media Authority, 'Consumer Information: Anti Spam - Reporting, Complaints, Enquiries' <http://www.acma.gov.au/ACMAINTER.65690:STANDARD:836464639:pc=PC_1970 > at 21 November 2005.

47 Hughes, above n 41, 42.

48 Goldman, above n 28, 5.

49 Ibid.

50 Ibid.

51 Ibid.

52 Commonwealth, above n 6, 1.

53 Hong Kong Internet Service Providers Association, 'HKISPA Response to the Consultation Paper on the Proposals to Contain the Problem of Unsolicited Electronic Messages' (25 October 2004) 6.

54 Spam Act sch 2 ss 2, 4(2).

55 CAN-SPAM Act § 3(17).

56 Commonwealth, above n 6, 1.

57 Commonwealth, above n 6, 22.

Please give me a Privacy Card

Andrew Perry, legal.consult Pty Limited

Andrew Perry is a Director, Legal & Technology for legal.consult Pty Limited. He is also the President of the Committee for the New South Wales Society for Computers & Law.

The issue of an Australia Card briefly raised its head again this year, following the London terrorist bombings committed by British citizens.

There is no question that times have changed since the Australia Card debate swept Australia in the early 80's. Australians, like the citizens of many other western countries, are far more willing to trust their government with powers that impinge civil liberties generally, and privacy in particular.

On 10 May 2005, the Attorney General and Minister for Justice and Customs announced the allocation of $5.9 million over two years in the 2005-6 budget, "to initiate the development of a national identity security framework that is strong, comprehensive, consistent and interoperable".[1]

While the amount of funding is relatively small, the purpose of this funding is significant. The funding will be used for two pilot projects that will have clear implications for privacy in Australia.

The first project is known as the on-line document verifications service (**DVS**) pilot. The DVS pilot involves the development of a prototype system that can be used by the Department of Immigration and Multicultural and Indigenous Affairs (**DIMIA**) and the Department of Foreign Affairs and Trade (**DFAT**) to check the accuracy of government documents presented to them against existing government databases including DIMIA, DFAT, drivers licence and births, deaths and marriages (**BDM**) databases.[2]

The stated goal of the DVS pilot is to test the effectiveness of online, real-time document verification in reducing the time and improving the accuracy of validating identity documents.[3] It is proposed as part of the Government's strategy for "A Safer Australia."

The Minister and Attorney General have sought to reduce concerns regarding the privacy implications of the DVS with an assurance that the system will:

(a) only validate with a "yes" or "no" the information contained in the document provided by the individual;

(b) not allocate an identifying number; and

(c) not store personal details on a database.[4]

These reassurances reflect the outcry in the 80's over the prospect of government agencies using a common identifier such as an Australia Card number to identify individuals and thereby create a large intelligence database using data matching.

Ironically, despite the apparent recognition of the Australia Card debate in the DVS pilot, the second project being funded from the 2005-6 Budget is the "Accuracy of data on an Australian Government database pilot" (**Data Matching Pilot**).[5]

The Data Matching Pilot will test the accuracy of 25,000 Australian Tax Office records through cross-agency data matching against DIMIA, DFAT, BDM, Health Insurance Commission, Australian Electoral Commission, Centrelink and drivers licence databases.[6]

The objective of the Data Matching Pilot is said to be identifying "key data matching elements that can be used to improve the accuracy of personal information held on a government database to identify false identities and inaccurate records."[7] In layman's terms, this could be interpreted to mean "finding the personal information we can use to link our key identity databases in the absence of an identity number."

The likely and apparently intended consequence of these two pilots is that the Australian Government will be able to correlate information about individuals and validate their identity in essentially the same way as if they were each required to provide a single identification number when dealing with government agencies.

So where is the public outcry that accompanied the proposal for an Australia Card in the 80's? Are these projects simply under the radar of the average Australian?

The lack of any significant public campaign against these projects or the new ePassports containing biometric information[8], suggests there has been a fundamental shift in the way Australians perceive government. Australians now appear willing (or resigned) to trust the government with all the personal information held by various departments in the name of protecting them from the 'evildoers' engaged in organised crime and terrorism, in particular.

Anti-Money Laundering developments

The Federal Government is expected to soon release an exposure draft of the Anti-Money Laundering and Counter Terrorist Financing Bill (**AML Bill**) to implement the 40 recommendations made by the Financial Action Task Force on Money Laundering (**FATF 40 Recommendations**).

The FATF 40 Recommendations were made following the events of September 11, 2001. Among other things, they recommend that a large number of private organisations be required to conduct customer due diligence (**CDD**) when establishing a business relationship and when specific trigger events occur.[9]

The AML Bill will be introduced in two tranches and is expected to require private organisations such as financial institutions, casinos, bullion dealers, lawyers, accountants, jewellers and real estate agents to verify their customers' identities from reliable, independent source documents as part of the CDD process.[10] In order to prove their compliance, these organisations will likely need to retain a copy of the relevant documents.

It is widely expected that the CDD requirements under the AML Bill will be more stringent than the "100-point ID Check" imposed under the *Financial Transaction Reports Act* 1988 *(Cth)*. In light of the Government's DVS pilot, it is possible that the private organisations required to undertake CDD will be given access to the DVS in order to validate the authenticity of the identity documents presented to them.

While financial institutions are experienced in conducting a "100-point ID Check", the expected changes to the CDD procedure under the AML Bill will still have a substantial cost to the finance industry. The other private organisations expected to be regulated by the AML Bill for the first time, on the other hand, will have negligible experience in conducting identity checks and many, such as small real estate agents, jewellers, lawyers and accountants, are likely to be small businesses operators for the purposes of the *Privacy Act* 1988 *(Cth)* (**Privacy Act**). Specific privacy obligations may need to be imposed on these organisations under the AML Bill or through amendments to the Privacy Act in order to protect the privacy of personal information contained in identity documents.

The privacy implications of a large number of private organisations holding copies of identity documents can be illustrated by the Bank of America's experience. In December 2004, the bank lost customer data for 1.2 million accounts of federal employees, including US Senators.[11] The data was contained on computer backup tapes and included social security numbers and account information that could reportedly enable identity theft.

The prime suspects in the disappearance of the backup tapes were baggage handlers, leading US Senator Charles Schumer to remark, "Whether it is identity theft, terrorism, or other theft, in this new complicated world baggage handlers should have background checks and more care should be taken for who is hired for these increasingly sensitive positions".[12]

If organisations with the resources of the Bank of America face difficulty maintaining security over identity information, it is unlikely that small organisations required to conduct CDD under the AML Bill will be able to do so.

The Privacy Commissioner's View

In her review of the private sector provisions of the Privacy Act,[13] the Privacy Commissioner has highlighted the inconsistencies that have emerged in privacy regulation due to a combination of the separate privacy principles governing the public and private sector, the heightened security environment following September 11 and developments in technology.[14]

The Privacy Commissioner has recommended the commissioning of a systematic examination of the Information Privacy Principles and the National Privacy Principles with a view to developing a single set of principles applicable to both public and private sector organisations.[15]

The private sector's increasing involvement in government activities, including government contracting and reporting of money laundering, and the government's involvement in commercial enterprise[16] and the implementation of DVS and data matching systems, means that a transparent and consistent privacy protection regime is needed.

So just give me a Privacy Card!

Given the inherent privacy risks with giving copies of credit card, medicare card, passport, drivers licence, birth certificate and other documents to

banks, bullion dealers, jewellers, accountants, real estate agents and lawyers, an Australia Card could actually protect the privacy of individuals. Consequently, politicians and bureaucrats concerned by the baggage attached to the "Australia Card" might like to consider a "Privacy Card" as a more palatable alternative for the new device.[17]

Rather than allow photocopies of their identity documents to be made, individuals could simply present a smart card (Privacy Card) containing a digitally signed picture of themselves that could be inserted into a card reader and validated online against the appropriate secure government database. Instead of an organisation obtaining a copy of numerous identity documents containing personal information that is irrelevant to the transaction, the Privacy Card verification system could output only a confirmation of the personal information that the requesting organisation requires for the transaction and which it is legally and contractually bound to protect.

If an individual is setting up a company or bank account, why should their lawyer or banker need their passport number, drivers licence number and credit card or medicare card number on file if an online system can simply validate the accuracy of the photo, name, address and date of birth the card holder has provided?

The emergence of digital certificates and an online DVS since the last Australia Card debate means that the implementation of a Privacy Card need not involve issuing every Australian with a single identity number, reminiscent of the holocaust. By enabling specific government agencies and private sector organisations with anti-money laundering responsibilities to validate a Privacy Card online, those agencies and organisations need only retain a copy of the personal information relevant to the particular transaction, together with a copy of the validation given to those details by the DVS system.

A Privacy Card need not allocate individuals with a single certificate that, like an identity number, would be their electronic identity for life. It is usual for digital certificates to have a defined life span. Every few years, or when a card is lost or stolen, the old digital certificate would become invalid and individuals would be issued with a new digital certificate that only authorised agencies and organisations could link to the individual's identity information and the previous certificate. Under this regime, as soon as an individual's wallet is stolen, the person could notify the applicable government agency to cancel the Privacy Card, and by presenting appropriate evidence to a government agency, such as Australia Post, a new card could be promptly obtained. If the thief tried to use the stolen Privacy Card, the online DVS would identify it as stolen.

The major concern such a system would create is the ability of private sector organisations to access government databases. This process raises fears that these private sector organisations could access a wealth of government personal information, including sensitive health information. This concern, however, can be addressed technically by ensuring that the database being accessed by private sector organisations only contains the relevant subset of an individual's identity information. If necessary for public confidence, the legislative framework could also impose additional criminal penalties for breaching or attempting to breach the security surrounding government held personal information.

While a Privacy Card would create efficiencies by standardising the identification process used by public and private sector organisations, the challenge for government and private sector proponents is to convince Australians that the card would also increase privacy, rather than reduce it. Since the Government's budget allocation to data matching and a DVS pilot has hardly raised an eyebrow, now might just be the time to try.

---

1 "Identity Security Strengthened", Joint News Release, Attorney General The Hon Philip Ruddock MP and Minister for Justice and Customs The Hon Senator Christopher Ellison, 10 May 2005.

2 "A Safer Australia", 2005-6 Budget Paper, The Attorney General's Portfolio, undated, p7.

3 Ibid.

4 "Identity Security Strengthened", op. cit.

5 Ibid.

6 Ibid.

7 Ibid.

8 The ePassport was launched on 24 October 2005 and has an embedded microchip storing the passport holder's digitised photograph, name, gender, date of birth, nationality, passport number and the passport expiry date. See http://www.dfat.gov.au/dept/passports/ for more information.

9 "The Forty Recommendations", Financial Action Task Force on Money Laundering, 20 June 2003 (incorporating the amendments of 22 October 2004).

10 "Government strengthening anti-money laundering and counter-terrorist financing", Media Release, Minister for Justice and Customs The Hon Senator Christopher Ellison, 11 October 2005.

11 "Bank of America loses customer data", The Associated Press, http://www.msnbc.msn.com/id/7032779

12 Ibid.

13 "Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988", Office of the Privacy Commissioner, Australian Government, March 2005.

14 Ibid, p4.

15 Ibid, p8.

16 Ibid, pp33, 39.

17 While the "ePassport" may become a de facto Australia Card, the embedding of additional information in the ePassport makes it less private than the Privacy Card discussed in this article and it would be necessary to issue a different device to non-travelling citizens and non-citizen residents.